APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/287,654	04/07/1999	PATRICK W. DOWD	DOWD-3-3	6548

27973   7590   02/13/2003

OFFICE OF THE ASSOC. GEN. COUNSEL (IP & T)
9800 SAVAGE ROAD SUITE 6542
FORT MEADE, MD   20755-6542

EXAMINER
REVAK, CHRISTOPHER A

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 02/13/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
     closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

   4a) Of the above claim(s) <u>27</u> is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4-8,14 and 17-21* is/are rejected.

7)☒ Claim(s) *2,3,9-13,15,16 and 22-26* is/are objected to.

8)☒ Claim(s) <u>27</u> are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

       1.☐ Certified copies of the priority documents have been received.

       2.☐ Certified copies of the priority documents have been received in Application No. _____ .

       3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
            application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

14)☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)   4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)   5) ☐ Notice of Informal Patent Application (PTO-152)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *5,6* .   6) ☐ Other: .

DETAILED ACTION

Election/Restriction

1.   Restriction to one of the following inventions is required under 35 U.S.C. 121:

I.   Claims 1-26 are drawn to allowing/discarding connectionless network packets based on whether are on an approved/disapproved list, classified in class 713, subclass 201. The disclosed subject matter falls under the subclassification because the criteria states "means or steps for providing system security at network level."

II.   Claim 27 is drawn to connecting various devices to an input/output bus, classified in class 710, subclass 100. The disclosed subject matter falls under the subclassification because the criteria states "means or steps for interconnecting or communicating between two or more components connected to an interconnection medium (e.g., a bus) within a single computer or digital data processing system."

2.   Inventions are distinct from each other and are related because of the following reasons: Inventions I and II, are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct from each other if they are shown to be separately usable. In the instant case, invention I is drawn towards allowing/discarding connectionless network packets based on whether are on an approved/disapproved list wherein invention II recites connecting various devices to an input/output bus. See MPEP § 806.05(d).

3.   Because these inventions are distinct for the reasons given above and the search required

for Group I is not required for Group II, restriction for examination purposes as indicated is

proper.

4.   During a telephone conversation with Robert Morelli on January 9, 2003 a provisional

election was made without traverse to prosecute the invention of Group I, claims 1-26.

Affirmation of this election must be made by applicant in replying to this Office action. Claim 27

is withdrawn from further consideration by the examiner, 37 CFR 1.142(b), as being drawn to a

non-elected invention.

Information Disclosure Statement

5.   The information disclosure statement submitted is in compliance with the provisions of 37

CFR 1.97. Accordingly, the information disclosure statement is being considered by the

examiner.

Priority

6.   Applicant's claim for domestic priority under 35 U.S.C. 119(e) is acknowledged.

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

8.   Claims 1,4-8,14, and 17-21are rejected under 35 U.S.C. 103(a) as being unpatentable over

Decasper et al in view of Coley et al.

As per claims 1 and 14, it is disclosed by Decasper et al of monitoring IPv6

(connectionless) packet whereby an association identification unit or AIU (database) stores

information pertaining to a flow of data (connectionless) data packets and additionally stored filter

information (rules). A received IPv6 (connectionless) packet is associated with an identifier (flow

tag). If the (connectionless) packet includes an unknown flow, a new flow entry is automatically

created (computed) for it which is added to and stored in the AIU (database comprising an

approved list) and it is allowed to pass (pg 4 & 5). On pg 4 it is recited that the AIU (database)

is used for flow detection which the examiner asserts that incoming identifiers (flow tags) are

compared to (approved) data previously stored whereby a match is performed and the IPv6

(connectionless) packet is allowed to pass. It is inherent that teachings of Decasper et al initialize

the AIU (database) since it is necessary for relationships and data types are defined beforehand so

that queries and manipulation of the data can be accomplished more efficiency. The teachings of

Decasper et al are silent in disclosing of a disapproved list which contains information on

connectionless packets which should be discarded. It is disclosed by Coley et al of monitoring

incoming IP (connectionless) packets and to determine the validity of the source address (col. 8,

lines 1-3 and col. 11, lines 47-48). If the analyzed source address is compared against authorized

(approved list) and unauthorized (disapproved list) addresses maintained by a proxy agent (which

is stored in a database) and the comparison includes checking if the source is unknown, if it is not

on the list, then it is denied (col. 11, lines 22-32). It would have been obvious to a person of

ordinary skill in the art at the time of the invention to have been motivated to apply a means of

discarding unauthorized information that may provide harmful effects to a computer. The

motivation of Coley et al is that problems in the prior art exist when a packet comprises an

unknown address and because it is not identified, it is allowed to pass (col. 3, lines 11-14) and this

presents a problem because it provides the hacker a means to bypass the packet filter (col. 3, lines

21-22). Coley et al utilizes the source address information whereby the flow tag information of

Decasper et al discloses that the source address is included within the flow (pg 4). The teachings

of Decasper et al would have benefitted from the teachings of Coley et al as a means to block

unknown packets which are not listed as authorized (approved) or unauthorized (disapproved)

and ultimately protect their computer from an attack whereby conventional packet filtering

techniques would have allowed the packet to be passed.

As per claims 4 and 17, Coley et al is relied upon for monitoring incoming IP

(connectionless) packets and to determine the validity of the source address (col. 8, lines 1-3 and

col. 11, lines 47-48). If the analyzed source address is compared against authorized (approved

list) and unauthorized (disapproved list) addresses maintained by a proxy agent (which is stored in

a database) and the comparison includes checking if the source is unknown, if it is not on the list,

then it is denied (col. 11, lines 22-32).

As per claims 5 and 18, Decasper et al teaches of receiving IPv6 (connectionless) packets

which is associated with an identifier (flow tag). If the (connectionless) packet includes an

unknown flow, a new flow entry is automatically created (computed) for it which is added to and

stored in the AIU (database comprising an approved list) and it is allowed to pass (pg 4 & 5). On

pg 4 it is recited that the AIU (database) is used for flow detection which the examiner asserts

that incoming identifiers (flow tags) are compared to (approved) data previously stored whereby a

match is performed and the IPv6 (connectionless) packet is allowed to pass.

As per claims 6 and 19, the teachings of both Decasper et al and Coley et al are silent in

disclosing of recording all allowances of access to the information protection network and

recording all discarded connectionless (IP) packets. The examiner hereby takes official notice that

such a concept is notoriously well known in the art. It would have been obvious to a person of

ordinary skill in the art at the time of the invention to have been motivated to apply an event log

which records all actions that have occurred whereby specific information is stored by type. It is

notoriously well known that logs record various information for use by a user or system

administrator for later reference in case if the information is desired to be viewed and interpreted.

For purposes of auditing, a user or administrator can access the information and analyze the

patterns to see the rate of usage to determine the events which led up to a situation such as an

attack. Certain packets that are either approved or disapproved would be recorded in the event

log and it can be figured out in what manner they have been sent. In the case of Coley et al, this

would have been beneficial to the teachings for an attack could have been analyzed so that it

could be learned how the attack occurred and future attacks can be detected more easily based on

viewing the results as recorded in an event log.

As per claims 7,8,20, and 21, the teachings of both Decasper et al and Coley et al are

silent in disclosing of alerting a system administrator if the number of discarded IP packets exceed

just a user-definable threshold or a user definable threshold within a user definable span of time.

The examiner hereby takes official notice that such a concept is notoriously well known in the art.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to

have been motivated to alert an administrator if a threshold is reached over a specific time period.

It is notoriously well known that the packet rate of transfers vary based on certain times of the

days, whereby there will be peak performance times over certain periods. Allowing a user-

definable threshold or a user definable threshold within a user definable span of time would allow

the user to determine the effectiveness of triggering an alert to an administrator about the

threshold being reached. Certain attacks such as a denial of service attack flood the system with

many packets and overwhelm it because all the packets cannot be processed due to exceeding

capacity. A threshold value would have to be determined which considers normal packet transfers

over peak and off-peak hours, but would effective determine an attack such as a denial of service

attack whereby the administrator would be alerted.

Allowable Subject Matter

9.   Claims 2,3,9-13,15,16, and 22-26 are objected to as being dependent upon a rejected base

claim, but would be allowable if rewritten in independent form including all of the limitations of

the base claim and any intervening claims.

Conclusion

10.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

Robins et al, U.S. Patent 6,430,184

Spinney et al, U.S. Patent 6,426,943

Spinney et al, U.S. Patent 6,226,267

Dowd et al, U.S. Patent 6,141,755

Maria et al, U.S. Patent 6,092,110

Boswell et al, "Support for Heterogeneous Communication Infrastructures in the HLA

RTI"

"Is IPv6 in trouble? An analysis of IPv6 solutions to the IPv6 features"

11.   Any inquiry concerning this communication or earlier communications from the examiner

should be directed to Christopher Revak whose telephone number is (703) 305-1843. The

examiner can normally be reached on Monday-Thursday from 6:30 am to 4:00 pm. The examiner

can also be reached on alternate Fridays from 6:30 am to 3:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor,

Gail Hayes, can be reached on (703) 305-9711. The fax phone number for the organization where

this application or proceeding is assigned as follows:

for After-Final Communications:	(703) 746-7238;
for Official Communications:	(703) 746-7239;
for Non-Official Communications:	(703) 746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding

should be directed to the receptionist whose telephone number is (703) 305-3900.

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

CR

February 4, 2003